October 27, 2015

A cyber war might be closer than we think

Book looks at how the U.S. military's rush to develop technology leaves security in the dust

FEATURED STORY BY RODIKA TOLLEFSON, THIRDCERTAINTY

How well prepared is the U.S. military for all-out network-centric warfare?

Not very, argues Richard Stiennon, a renowned cybersecurity analyst, in his latest book, "There Will Be Cyberwar: How the Move to Network-centric War Fighting Has Set the Stage for Cyberwar."

The Pentagon remains much too dependent on vulnerable, constantly targeted, off-the-shelf operating systems. And even as new, more secure systems get introduced, the majority of the Defense Department's infrastructure still runs on outdated Windows and other vulnerable software.

Infographic: *Can U.S. cyber sanctions chill attacks?*

Stiennon, founder of consultancy IT-Harvest and former vice president of research at Gartner Inc., an information technology and research firm, says the Pentagon needs to overhaul its encryption-key management systems, harden the supply chain against disruptions, and scrutinize all related software.

ThirdCertainty recently sat down with Stiennon to drill down on his hypotheses. (Answers edited for length and clarity.)

ThirdCertainty: You point out that the cyber 911analogy often used in the media and defense sector is incorrect and that an attack on the military is more like a cyber Pearl Harbor. How are the two different?

Stiennon: An attack against the power grid and communication systems that everyone talks about and will send us to the Dark Ages would be much more akin to a terrorist attack, with no strategic advantage other than to take out "the big evil empire." While you'd take out the infrastructure before invading a country, that's not a likely scenario in the United States' case.

Cyber Pearl Harbor is a surprise attack on the military thanks to information dominance. You can jam all the radars, take over communications, and use all the techniques I talk about in the book. That's where I drew the analogy, starting with the crisis in the Taiwan Straits and building on that as an example of how that could develop into a future crisis, with the United States losing the military engagement.

3C: Both scenarios sound plausible. Which is more likely to happen?

Richard Stiennon, author and IT-Harvest founder

Stiennon: Terrorism is not warfare and it's much harder to get a grip on, but nation-states battling for dominance in the global economy is pretty easy to understand. You have 400 years of history of that. In the future, there will be military clashes between major powers. I can say with complete assurance that future wars will involve cyber attacks. The powers that have the best chance of winning the battles are the ones that have information dominance.

And yes, we're completely vulnerable to a devastating attack on U.S. infrastructure. It's completely possible to do, and it wouldn't cost very much. All you need now is a bad actor who wants to do it.

3C: If the military took all the steps you recommend in the book, would it fix all its problems?

Stiennon: When I answer the question, "What should be done," I imagine the path that will be taken after the disaster occurs. Imagine, as I've done in the book, losing a major military confrontation with loss of life, loss of equipment, and loss of prestige on the global scene, how would you have prevented that?

One, you would have done a much better job of protecting your critical weapons design systems to keep them from being stolen by China. Now we know they have our designs, and

probably our source code, and they know all the vulnerabilities in it. We should fix the vulnerabilities, protect those systems with additional layers of security, and start worrying seriously about the supply chain of all of our components.

3C: Is the military doing anything differently now and paying attention to its cyber vulnerabilities?

Stiennon: There's now discussion about the vulnerabilities and an interest in doing something about it. But in the military, that means we're 10 years away from everything being baked into operations.

3C: So things are moving in the right direction, though in the meantime the threat is still there?

Stiennon: They're moving in the right direction but, unfortunately, all the military platforms are frozen in time, and they don't update them regularly to improve them. From here on out, new systems should have security built in.

Posted in Featured Story